					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P03S					Titolo del documento: **Politica sull'uso accettabile**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Allineamento a norme e regolamenti, ove applicabile

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 5	Rilevante per l'ambito complessivo di applicazione della politica e per la sua attuazione
ISO/IEC 27002:2022	5.10, 5.11, 5	Fornisce linee guida sui requisiti e sui controlli relativi all'uso accettabile dei beni aziendali
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Copre l'uso di sistemi e dispositivi, il monitoraggio e la formazione degli utenti
GDPR UE	Articoli 5(1)(f), 32	Integrità e riservatezza dei dati e misure di sicurezza
NIS2 UE	Articolo 21(2)(b)	Richiede politiche di sicurezza e di uso accettabile adeguate
DORA UE	Articolo 9	Politica di gestione del rischio ICT, controlli e applicazione
COBIT 2019	DSS05, BAI	Servizi di sicurezza e gestione della conoscenza

1. Scopo

1.1. La presente politica definisce l'uso accettabile, responsabile e sicuro dei sistemi, dei dispositivi, dell'accesso a Internet, della posta elettronica, dei servizi cloud e di eventuali dispositivi personali utilizzati per finalità aziendali.

1.2. Essa garantisce che i soggetti interessati comprendano i propri obblighi nell'utilizzo delle risorse IT dell'organizzazione, tutelando l'integrità dei dati, la riservatezza e la continuità operativa.

1.3. La presente politica supporta la conformità alla ISO/IEC 27001:2022 definendo chiari standard di comportamento per gli utenti, in linea con i requisiti legali, contrattuali e normativi.

2. Ambito di applicazione

2.1. La presente politica si applica a tutti i soggetti che accedono ai sistemi aziendali o ai dati, li gestiscono o interagiscono con essi, inclusi:

2.1.1. dipendenti e collaboratori esterni

2.1.2. lavoratori temporanei o tirocinanti

2.1.3. fornitori esterni di servizi IT

2.2. La politica si applica a:

2.2.1. computer, telefoni e tablet di proprietà aziendale

2.2.2. dispositivi personali approvati per l'uso aziendale (BYOD)

2.2.3. reti aziendali, piattaforme cloud e servizi software

2.2.4. accesso a Internet, sistemi di posta elettronica, archiviazione condivisa e applicazioni aziendali

2.3. La presente politica si applica in tutti gli ambienti di lavoro, in sede, da remoto e ibridi, e per tutta la durata delle attività aziendali.

3. Obiettivi

3.1. Definire cosa costituisce un uso accettabile e non accettabile dei sistemi IT.

3.1.1. Ridurre i rischi per la sicurezza derivanti da uso improprio, accesso non autorizzato o introduzione di malware.

3.1.2. Proteggere i dati aziendali, le informazioni dei clienti e la reputazione dell'azienda.

3.1.3. Stabilire regole vincolanti e garantire la responsabilizzazione di tutti gli utenti.

3.1.4. Supportare il monitoraggio e la conformità per rilevare tempestivamente le violazioni e adottare azioni correttive.

4. Ruoli e responsabilità

4.1. Direttore generale (GM)

4.1.1. Approva la presente politica ed è responsabile di garantire la disponibilità delle risorse e dell'autorità necessarie per la sua applicazione.

4.1.2. Riesamina e autorizza eventuali eccezioni alla presente politica.

4.2. Responsabile IT o fornitore esterno di supporto IT

4.2.1. Mantiene gli inventari del software e dell'hardware approvati.

4.2.2. Configura i dispositivi per applicare le regole di uso accettabile, ad esempio mediante filtraggio dei contenuti e registrazione degli accessi.

4.2.3. Monitora l'utilizzo per individuare potenziali violazioni e indaga sugli incidenti.

4.2.4. Garantisce che i dispositivi personali (BYOD), se utilizzati per finalità aziendali, siano autorizzati e sicuri.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Requisiti di riesame e aggiornamento

9.1. Riesame annuale

9.1.1. La presente politica deve essere riesaminata annualmente dal Responsabile IT, con approvazione finale del Direttore generale (GM), per garantire che resti allineata alle modalità di utilizzo della tecnologia, ai rischi emergenti e agli obblighi di conformità.

9.2. Fattori attivanti per il riesame intermedio

9.2.1. I riesami devono inoltre essere effettuati in risposta a:

9.2.2. nuovi sistemi o tecnologie, ad esempio un nuovo servizio cloud o una nuova piattaforma endpoint

9.2.3. violazioni significative della politica

9.2.4. aggiornamenti normativi o modifiche contrattuali che incidono sull'uso dell'IT

9.3. Documentazione delle modifiche

9.3.1. Tutti gli aggiornamenti devono essere registrati in un registro delle modifiche che includa:

9.3.1.1. numero di versione

9.3.1.2. data del riesame

9.3.1.3. sintesi delle modifiche

9.3.1.4. autorità approvante

9.4. Comunicazione della politica

9.4.1. Le versioni aggiornate della presente politica devono essere condivise con tutti gli utenti interessati. I dipendenti devono confermare la ricezione e la comprensione nell'ambito dei propri obblighi di sensibilizzazione alla sicurezza.

10. Politiche correlate e collegamenti

10.1. La presente politica opera congiuntamente ad altre politiche SME per garantire una copertura completa delle responsabilità di sicurezza:

10.1.1. P4S – Politica per il controllo degli accessi: definisce l'attuazione tecnica e procedurale dell'uso consentito e delle restrizioni sugli account.

10.1.2. P8S – Politica di sensibilizzazione e formazione sulla sicurezza delle informazioni: fornisce agli utenti formazione sui limiti dell'uso accettabile e sugli obblighi di segnalazione.

10.1.3. P9S – Politica sul lavoro da remoto: disciplina l'uso dei sistemi aziendali in ambienti esterni alla sede o domestici.

10.1.4. P17S – Politica di protezione dei dati e privacy: applica le regole di trattamento dei dati personali che interagiscono con il monitoraggio dell'uso accettabile e con il BYOD.

10.1.5. P30S – Politica di risposta agli incidenti: disciplina le procedure per l'indagine e la risposta a usi impropri o violazioni delle condizioni di uso accettabile.

11. Norme e quadri di riferimento

11.1. ISO/IEC 27001

11.1.1. Controllo 5.10 – Richiede alle organizzazioni di definire e applicare l'uso accettabile dei beni informativi aziendali.

11.2. ISO/IEC 27002

11.2.1. Controllo 5.10 – Fornisce linee guida sull'uso accettabile dei sistemi, inclusi i comportamenti consentiti e vietati.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Riguarda il controllo dell'uso dei sistemi, inclusi i dispositivi personali.

11.3.2. AC-20 – Richiede l'autorizzazione e il monitoraggio dei sistemi esterni.

11.3.3. AT-2 – Sottolinea la formazione degli utenti sulle pratiche di uso accettabile.

11.4. GDPR UE

11.4.1. Articolo 5(1)(f) – Richiede l'integrità e la riservatezza dei dati personali, che possono essere compromesse da usi impropri da parte degli utenti.

11.4.2. Articolo 32 – Richiede l'attuazione di misure tecniche e organizzative per proteggere sistemi e dati.

11.5. NIS2 UE

11.5.1. Articolo 21(2)(b) – Richiede politiche di sicurezza adeguate, incluse regole sull'uso accettabile, per mitigare le minacce cyber.

11.6. DORA UE

11.6.1. Articolo 9 – Richiede politiche di gestione del rischio ICT, che includano controlli sull'utilizzo e meccanismi di applicazione.

11.7. COBIT 2019

11.7.1. DSS05 – Gestire i servizi di sicurezza: pone l'accento sul controllo del comportamento degli utenti basato sulle politiche.

11.7.2. BAI08 – Gestire la conoscenza: tratta la consapevolezza delle responsabilità previste dalle politiche e la formazione sull'uso accettabile.